UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,986	01/18/2006	Satoshi Niwano	2005_1909A	7145

52349 7590 06/15/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
RAAB, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2156	

MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,986	NIWANO ET AL.	
	Examiner	Art Unit	
	Christopher J. Raab	2156	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *85-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *85-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

01. This action is in response to Applicant's amendment filed on **03/04/09**. **Claims 85 – 95** are pending in the present application. **This action is made FINAL**, as necessitated by amendment.

Claim Rejections - 35 USC § 101

02. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

03. **Claim 93** is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per **claim 93**, the claim recites a terminal apparatus comprising a receiving unit and a judging unit. The claim lacks the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101, and is understood by one of ordinary skill in the art to be software *per se*. It is clearly not a series of steps or acts to be a process nor is it a combination of chemical compounds to be a composition of matter. As such, it fails to fall within a statutory category. It is, at best, functional descriptive material per se.

Claim Rejections - 35 USC § 103

04. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

05. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

06. **Claims 85, and 90 – 95** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muntz et al. (US PGPub 2003/0208681)**, hereinafter 'Muntz', in view of **Doherty et al. (US Patent 6,920,567)**, hereinafter 'Doherty'.

Consider **claim 85**, Muntz discloses a method for controlling a terminal apparatus (paragraph [0013]), comprising:

a network (read as the terminal apparatus being connected to a network) (Fig. 1);

servers that store files accesses by file services (read as a content distribution server storing content and a content provided ID) (paragraph [0013]);

a metadata server that contains information about the files that are to be accesses (read as a metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata) (paragraph [0015]);

servers, including a block server, that can authenticate a user, which may use keys that can help connect a validated user to proper server for distributing the files (read as the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate) (Fig. 2, paragraphs [0021] – [0029]);

the user making the request for the file and receiving, as a result of the server interaction, the file, metadata, and key information, as it relates to the client transaction over the network (read as receiving, at the terminal apparatus, the content and the content provider ID stored in the content distribution server, receiving, at the terminal apparatus from the metadata distribution server, the metadata, receiving, at the terminal apparatus, the public key certificate generated by the authentication server) (paragraphs [0030] – [0040]).

Although Muntz discloses controlling how to obtain the files from the servers, Muntz does not specifically disclose a license management server, which can help authenticate a user requesting file access.

In the same field of endeavor, Doherty discloses a method, comprising:

a license server can be used to determine whether a user has the access right to files (read as the license management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus) (column 2 lines 37 – 61);

using the license information obtained in order to determine if a user has the appropriate privileges with respect to the requested software usage or access (read as judging, at the terminal apparatus, whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server, judging, at the terminal apparatus, whether the received content provider ID matches the certificate signer ID included in the public key certificate, when it is judged that the content provider ID does not match the metadata signer ID) (column 3 line 56 – column 4 line 62);

allowing for the data to be transferred upon successful authentication of the user license (read as determining, at the terminal apparatus, that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID) (column 5 line 47 – column 6 line 48).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the license creation and authentication taught by

Doherty into the content distribution server network taught by Muntz for the purpose of allowing further authentication means though licensing to be used as a way of controlling content distribution to users.

Consider **claim 90**, and **as applied to claim 85 above**, Muntz discloses a method such that metadata controls which permission the user has (read as the usage control information includes control permission information, the control permission information indicating whether the user metadata is permitted to be used, and the method further comprises judging whether the user metadata is permitted to be used based on the control permission information) (paragraphs [0016], [0023]).

Consider **claim 91**, and **as applied to claim 85 above**, Muntz discloses a method such that the metadata controls which users are given which permission, such that the information to be related to a user or a device used by a user (read as the user metadata is encrypted by a predetermined encryption key, wherein the usage control information includes control permission information, the control permission information indicating whether the user metadata is permitted to be used, wherein the usage control information includes moving range specifying information, the moving range specifying information indicating whether the user metadata is permitted to be moved out of the terminal apparatus, and wherein the method further comprises judging whether the user metadata is permitted to be used based on the control permission information) (paragraphs [0016], [0024], [0026]).

Consider **claim 92**, and **as applied to claim 91 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for

the user, and decrypting the information using a key (read as the predetermined encryption key comprises secret information common to one ore more terminal apparatuses owned by the user of the terminal apparatus) (paragraphs [0016], [0024], [0026]).

Consider **claim 93**, Muntz discloses a terminal apparatus (paragraph [0013]), comprising:

a network (read as the terminal apparatus being connected to a network) (Fig. 1);

servers that store files accesses by file services (read as a content distribution server storing content and a content provided ID) (paragraph [0013]);

a metadata server that contains information about the files that are to be accesses (read as a metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata) (paragraph [0015]);

servers, including a block server, that can authenticate a user, which may use keys that can help connect a validated user to proper server for distributing the files (read as the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also

including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate) (Fig. 2, paragraphs [0021] – [0029]);

the user making the request for the file and receiving, as a result of the server interaction, the file, metadata, and key information, as it relates to the client transaction over the network (read as receiving the content and the content provider ID stored in the content distribution server, receiving from the metadata distribution server, the metadata receiving the public key certificate generated by the authentication server) (paragraphs [0030] – [0040]).

Although Muntz discloses controlling how to obtain the files from the servers, Muntz does not specifically disclose a license management server, which can help authenticate a user requesting file access.

In the same field of endeavor, Doherty discloses a terminal apparatus, comprising:

a license server can be used to determine whether a user has the access right to files (read as the license management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus) (column 2 lines 37 – 61);

using the license information obtained in order to determine if a user has the appropriate privileges with respect to the requested software usage or access (read as judging whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information

indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server, judging whether the received content provider ID matches the certificate signer ID included in the public key certificate, when it is judged that the content provider ID does not match the metadata signer ID) (column 3 line 56 – column 4 line 62);

allowing for the data to be transferred upon successful authentication of the user license (read as determining that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID) (column 5 line 47 – column 6 line 48).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the license creation and authentication taught by Doherty into the content distribution server network taught by Muntz for the purpose of allowing further authentication means though licensing to be used as a way of controlling content distribution to users.

Consider **claim 94**, Muntz discloses a system (paragraph [0013]), comprising:

servers that store files accesses by file services (read as a content distribution server storing content and a content provided ID) (paragraph [0013]);

a metadata server that contains information about the files that are to be accesses (read as a metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the

metadata signer ID indicating a signer that digitally signs the metadata) (paragraph [0015]);

servers, including a block server, that can authenticate a user, which may use keys that can help connect a validated user to proper server for distributing the files (read as the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate) (Fig. 2, paragraphs [0021] – [0029]);

the user making the request for the file and receiving, as a result of the server interaction, the file, metadata, and key information, as it relates to the client transaction over the network (read as a terminal apparatus, comprising: a receiving unit for receiving the content and the content provider ID stored in the content distribution server, receiving from the metadata distribution server, the metadata receiving the public key certificate generated by the authentication server) (paragraphs [0030] – [0040]).

Although Muntz discloses controlling how to obtain the files from the servers, Muntz does not specifically disclose a license management server, which can help authenticate a user requesting file access.

In the same field of endeavor, Doherty discloses a terminal apparatus, comprising:

a license server can be used to determine whether a user has the access right to files (read as the license management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus) (column 2 lines 37 – 61);

using the license information obtained in order to determine if a user has the appropriate privileges with respect to the requested software usage or access (read as a judging unit for judging whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server, judging whether the received content provider ID matches the certificate signer ID included in the public key certificate, when it is judged that the content provider ID does not match the metadata signer ID) (column 3 line 56 – column 4 line 62);

allowing for the data to be transferred upon successful authentication of the user license (read as determining that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID) (column 5 line 47 – column 6 line 48).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the license creation and authentication taught by Doherty into the content distribution server network taught by Muntz for the purpose of allowing further authentication means though licensing to be used as a way of controlling content distribution to users.

Consider **claim 95**, Muntz discloses a computer-readable recording medium storing a program, the program controlling a terminal apparatus (paragraph [0013]), comprising:

a network (read as the terminal apparatus being connected to a network) (Fig. 1);

servers that store files accesses by file services (read as a content distribution server storing content and a content provided ID) (paragraph [0013]);

a metadata server that contains information about the files that are to be accesses (read as a metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata) (paragraph [0015]);

servers, including a block server, that can authenticate a user, which may use keys that can help connect a validated user to proper server for distributing the files (read as the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication

server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate) (Fig. 2, paragraphs [0021] – [0029]);

the user making the request for the file and receiving, as a result of the server interaction, the file, metadata, and key information, as it relates to the client transaction over the network (read as receiving, at the terminal apparatus, the content and the content provider ID stored in the content distribution server, receiving, at the terminal apparatus from the metadata distribution server, the metadata, receiving, at the terminal apparatus, the public key certificate generated by the authentication server) (paragraphs [0030] – [0040]).

Although Muntz discloses controlling how to obtain the files from the servers, Muntz does not specifically disclose a license management server, which can help authenticate a user requesting file access.

In the same field of endeavor, Doherty discloses a method, comprising:

a license server can be used to determine whether a user has the access right to files (read as the license management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus) (column 2 lines 37 – 61);

using the license information obtained in order to determine if a user has the appropriate privileges with respect to the requested software usage or access (read as

judging, at the terminal apparatus, whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server, judging, at the terminal apparatus, whether the received content provider ID matches the certificate signer ID included in the public key certificate, when it is judged that the content provider ID does not match the metadata signer ID) (column 3 line 56 – column 4 line 62);

allowing for the data to be transferred upon successful authentication of the user license (read as determining, at the terminal apparatus, that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID) (column 5 line 47 – column 6 line 48).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the license creation and authentication taught by Doherty into the content distribution server network taught by Muntz for the purpose of allowing further authentication means though licensing to be used as a way of controlling content distribution to users.

07. **Claims 86 – 89** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muntz et al. (US PGPub 2003/0208681)**, hereinafter 'Muntz', in view of **Doherty et al. (US Patent 6,920,567)**, hereinafter 'Doherty', in further view of **Lowe et al. (US PGPub 2004/0267693)**, hereinafter 'Lowe'.

Consider **claim 86**, and **as applied to claim 85 above**, Muntz, as modified by Doherty, discloses a method of generating metadata, but does not specifically disclose that metadata is generated by the user.

In the same field of endeavor, Lowe discloses a method such that the user can create and manage the metadata (read as the metadata comprises user metadata generated by a user of the terminal apparatus) (paragraphs [0017], [0069]).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the metadata management taught by Lowe into the user identification method taught for the purpose of allowing users to have control over the metadata.

Consider **claim 87**, and **as applied to claim 86 above**, Muntz discloses a method such that the user can be given full permission (read as the user metadata does not include the metadata signer ID) (paragraph [0023]).

Consider **claim 88**, and **as applied to claim 86 above**, Muntz discloses a method such that the metadata is encrypted, and that the user device holds the key (read as the user metadata in encrypted by secret information common to one or more terminal apparatuses owned by the user of the terminal apparatus) (paragraphs [0021], [0024], [0026]).

Consider **claim 89**, and **as applied to claim 85 above**, Muntz, as modified by Doherty, discloses a method for utilizing information, but does not specifically disclose that a user can create and modify the metadata.

In the same field of endeavor, Lowe discloses a method such that a user can have control over the metadata, by allowing the user to create, modify, and manage the metadata (read as the usage control information includes revision permission information, the revision permission information indicating whether the metadata is permitted to be revised, and the method further comprises judging whether the metadata is permitted to be revised based on the revision permission information, when it is determined that the metadata is available to the terminal apparatus.) (paragraphs [0017], [0069]).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the metadata management taught by Lowe into the user identification method taught for the purpose of allowing users to have control over the metadata.

Response to Arguments

08. Applicant's arguments with respect to claims 85 – 95 have been considered, but are moot in view of the new ground(s) of rejection.

Conclusion

09. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) Marconcini, Franco et al.	US Patent	6,834,110
b) Heutschi, Walter	US PGPub	2004/0176092

11. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450

Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

12. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Christopher Raab whose telephone number is (571) 270-1090. The Examiner can normally be reached on Monday-Friday from 8:30am to 6:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Pierre Vital can be reached on (571) 272-4215. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Christopher Raab
C.R./cr

June 09, 2009

/Pierre M. Vital/
Supervisory Patent Examiner, Art Unit 2156